REMARKS/ARGUMENTS

Remarks Concerning Amendments to Specification

The following informalities in the specification are corrected in accordance with the requirements set forth in the Action:

1. On page 9 of the specification, the label "308" for the "Control and Statistics Block" is corrected to read "314" as indicated in Figure 3.
2. On page 18 of the specification, the reference to "Multicast Meter 604" is corrected to read "Multicast Flood Meter 604" as indicated in Figure 6.
3. On page 20 of the specification, the reference to "Multicast Flood Meter 603" is corrected to read "Multicast Flood Meter 604" as indicated in Figure 6.

No new matter is added.

Remarks Concerning Amendments to Claims

Claims 1 and 8-10 are amended. Claims 4-7 and 11-20 are cancelled. New claim 21 is added.

Response to Objections to the Specification

Regarding the specification, the Office objected to three minor informalities in the disclosure. In response, Applicant amends the specification to address all the informalities pointed out in the Action.

Response to Claim Rejections — 35 USC § 112

Claims 8-10 and 18-20 were rejected under 35 USC 112 because the term "network characteristic" was considered vague and indefinite. Applicant responds by amending the claims to remove the term "network characteristics." The new language in the claims is supported in various portions of the specification, e.g., page 9, lines 6-17; page 29, lines 1-5 and 15-20; and page 31, lines 15-26.

Claims 1-9 and 12-20 were rejected under 35 USC 112 because it was unclear to the examiner whether the limitations of the claims were directed toward machine parts or software. Applicant responds by pointing out that the recited limitations are clearly physical components of a tangibly realized computing apparatus (e.g., the MAC interface recited in claim 1). Regarding various other limitations of claim 1, it is noted that computational components of a computing apparatus may be implemented not only as software but also in firmware or in hardware. Irrespective of the particular implementation of a given computational component, its physical realization in the computing apparatus constitutes a part of a computing apparatus or system, and is recited as such in the present claims. Such physical components may be characterized in terms of their functions. Thus, the physical components recited in the claims are not mere limitations to software but are rather limitations characterizing tangible components of the claimed computing apparatus or system.

Response to Claim Rejections — 35 USC § 101

Claims 1-10 and 11-20 were rejected under 35 USC 101 because the claims allegedly do not fall within a statutory category. In particular, the Office states in the Action that "each limitation of the claims is drawn towards software per se", and that "the claims are, at best, functional descriptive material per se." Applicant respectfully disagrees. Claim 1 is directed toward a digital computing apparatus and explicitly recites various physical components of such. For example, the first limitation of claim 1 recites a media access controller (MAC) interface, which is a physical component, and the second limitation recites a classification means operatively coupled to the MAC interface. These limitations are clearly physical in nature and can not be accurately or fairly characterized as "software per se" or "functional descriptive material per se." Accordingly, Applicant respectfully requests withdrawal of the rejection as being based on an incorrect reading of the claim language.

Response to Claim Rejections — 35 USC § 102 and § 103

Claims 1-5 and 7-20 were rejected under 35 USC 102(b) as being taught by US Patent Application Publication 2002/0032871 (herein after "Malan-1"). Claim 6 was rejected under 35 USC 102(b) as being taught by US Patent Application Publication 2002/0035698 (herein after

"Malan-2"). Applicant responds by amending the claims and demonstrating how the amended claims are clearly distinct and patentable over Malan-1 and Malan-2.

Applicant has amended claim 1 to include the limitations of claim 6 as well as intermediate claims 4 and 5. The Office alleged in the arguments against claim 4 that Malan-1 teaches in paragraph [0030] the claimed "SYN flood detection and prevention mechanism having a support means for creating a plurality of legitimate IP addresses during normal operation when the TCP state transitions to ESTABLISHED." The cited paragraph, however, does not teach the specific details recited in the claim. Although the paragraph mentions filtering mechanisms and filter list entries, it does not mention SYN flood detection, creating a plurality of legitimate IP addresses, or TCP state transitions to ESTABLISHED. Moreover, although Malan-1 refers to SYN-packet flood attacks in paragraph [0083], there is no teaching of the claimed "support means for creating a plurality of legitimate IP addresses during normal operation when the TCP state transitions to ESTABLISHED."

The Office alleged in the arguments against claim 5 that Malan-1 teaches in paragraph [0030] the claimed limitation that "said SYN flood detection and prevention mechanism allows only said plurality of legitimate IP addresses to be stored during normal operation." The cited paragraph, however, only speaks generally of filtering, and does not specifically teach any SYN flood detection mechanism, legitimate IP addresses, or the allowing of the legitimate IP addresses to be stored during normal operations.

The Office alleged in the arguments against claim 6 that Malan-2 teaches in paragraph [0066] the claimed zombie flood detection and prevention mechanism. The cited paragraph of Malan-2, however, refers only to TCP SYN floods as an example of a common type of denial of service that is removed by "a variety of safeguards" in the event that a request is new. There is no specific teaching in the cited paragraph of the claimed zombie flood detection and prevention mechanism. In particular, the paragraph does not teach the claimed "means for limiting connections to said plurality of legitimate IP addresses stored during normal operation" nor the claimed "means for determining a threshold for said connections based on baseline traffic learned during normal operation." It should be emphasized that the claimed technique has a means for limiting connections to *legitimate* IP addresses. In contrast, prior art techniques limit connections to *illegitimate* IP addresses.

Applicant has also amended claim 1 to include the limitations of claim 7. Although Malan-1 teaches a technique for tracing an attack across the network to its source [0077-0078], Malan-1 does not teach or suggest the claimed feature of "multiplicatively incrementing count for sources that send identified flood data."

As is evident from the above, although Malan-1 and Malan-2 disclose techniques and features with a vague resemblance to some aspects of the claimed invention, they do not teach many of the specific limitations recited in the claims. In addition, the prior art does not teach the surprising zombie flood detection and prevention mechanism that limits connections to *legitimate* IP addresses.

Applicant presents new claim 21 directed toward a computer-implemented method for rate-based denial of service attack detection. The claim recites several of the key distinguishing features discussed above in relation to claim 1 as amended. In particular, the claim recites (among other things) the unique zombie flood detection and prevention technique, including dropping packets from IP addresses in a table of legitimate IP addresses during a detected zombie flood state.

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

LUMEN I.P. SERVICES
2345 Yale Street, Palo Alto, CA 94306
(650) 424-0100

BY
Thomas J. McFarlane
Thomas J. McFarlane, Reg. No 39,299